UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,471	10/11/2001	James L. Jason JR.	10559-504001 / P11796	9923

20985 7590 11/09/2006

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
DIVECHA, KAMAL B	
ART UNIT	**PAPER NUMBER**
2151	

DATE MAILED: 11/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 09/976,471	**Applicant(s)** JASON ET AL.	
	Examiner KAMAL B. DIVECHA	**Art Unit** 2151	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 23 October 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: *none*.
   Claim(s) objected to: *none*.
   Claim(s) rejected: *1-46*.
   Claim(s) withdrawn from consideration: *none*.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: Please see the attached sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Response to Arguments

Claims 1-46 are pending in this application.

Applicant's arguments filed October 23, 2006 have been fully considered but they are not persuasive.

In response filed, applicant argues in substance that:

a. Chen does disclose each and every element of claim 1. For example, Chen fails to disclose "generating an average that relates to traffic of a specified type; comparing current network traffic to said average, at first and second points of a network… and based on said comparing analyzing the information generated" (remarks, page 12-17).

In response to argument [a], Examiner disagrees.

Chen clearly and/or explicitly discloses this functionality. Chen discloses a monitoring process that monitors the statistics of the network traffic flow at various point.

Chen's detection of the Dos attack based on the ratios is one aspect of the Chen's claimed invention.

Chen clearly indicates the process wherein gateway devices constantly analyze traffic, looking for congestion or traffic levels that indicate the onset of a DoS attack, wherein the data collectors are located inter alia at major peering points and network points of presence. The data collectors sample packet traffic, accumulate and collect statistical information about network flows (pg. 2 [0027]).

Furthermore, The data collectors as an example, maintains a log that specifies that the data collector has seen a certain number of packets, e.g. 10,000 packets of a particular kind, that apparently originated from a particular source that are going to a particular destination (pg. 3

[0037]). And, Based on rules within the data collector, the data collector analyzes the collected statistics and may if necessary compose a message that raises an alarm (pg. 3 [0038-0039]).

Furthermore, the gateways and data collectors keep statistical summary information of traffic over different periods of time and at different levels of detail. For example, a gateway may keep mean and standard deviation for a chosen set of parameters across a chosen set of time-periods. The parameters may include source and destination host or network addresses, protocols, type of packets, number of open connections or packets sent in either direction. Time periods for statistical aggregation may range from minutes to weeks. The device will have configurable thresholds and will raise warnings when one the measured parameters exceeds the corresponding threshold (pg. 6 [0079]).

The inclusion of the "parameters" and "statistics" as the parameters of interest in the above passage is evident that Chen's system is not limited to detection of DoS attack based on ratios only.

The fact that Chen does disclose the above subject matter can further be evidenced from APPENDIX B.

On page 27 of APPENDIX B, Chen discloses a GATHERRATES (N) component, which gathers aggregate traffic rates from TCPMonitor (n) element for various traffic type. Aggregate rates are gathered once every MONITOR_PERIOD number of seconds. They are averaged and saved to SAVE_FILE once every SAVE_PERIOD number of seconds.

On page 44 of APPENDIX B, Chen discloses a TCPMONITOR (n) component, which monitors and splits TCP traffic.

On page 35 of APPENDIX B, Chen discloses a RATEWARN (n) component, which is configured to monitor the rate of packet arrival on input port. Packets are forwarded to output port if rate is below RATE. If rate exceeds RATE, it sends out a warning packet.

In other words, the incoming traffic flow is compared to the RATE previously monitored or gathered, through the gatherrate (n) component that clearly recites that the rates are averaged.

Therefore, It is evident from the detailed mappings found in the above rejection(s) that Chen et al. disclosed this functionality, i.e. generating an average that relates to particular type or specified type and comparing network traffic to said average and based on comparison, analyzing the information. Further, it is clear from the numerous teachings (previously and currently cited) that the provision for the subject matter above was widely implemented in the networking art. Thus, Applicant's arguments drawn toward distinction of the claimed invention and the prior art teachings on this point are not considered persuasive.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAMAL B. DIVECHA whose telephone number is 571-272-5863. The examiner can normally be reached on Increased Flex Work Schedule.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung can be reached on 571-272-3939. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kamal Divecha
Art Unit 2151
November 6, 2006.

WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100